Cyber Threat Defender

THE CYBER SECURITY COLLECTABLE CARD GAME (Version 1.0)
Welcome to Cyber Threat Defender™, the cyber security collectable card game!!!!

The goal of the game is to increase the size of your network, thus obtaining more points each turn. While you are doing this, however, you must ensure that you build out your network in a secure manner. Adding a wireless router without using encryption will make your network vulnerable to attackers who can capture your traffic. Not using a firewall could mean that attackers hack into your systems. Inadequate user training might mean that your users fall for a phishing attack. These are just some of the possible events and attacks that can occur during your game so build your network wisely with security in mind!!!

Cyber Threat Defender was created as part of the Culture of Security Campaign at the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA). Its purpose is to provide a basic awareness of a number of security issues, such as those mentioned previously. There have been a number of security games created in the past, but frequently these games suffer from one of two major problems – individuals could play the game and come away without having learned anything about security, and most were simply just not fun. We have attempted to address both of these issues.

The collectable card game genre is a popular one and there are many games on the market that fall into this category. We have started with a basic starter deck and three booster packs. Each starter deck has the same basic cards but the booster packs will vary, thus allowing for two players to create their own unique deck for playing. Future plans include the creation of additional booster packs with new cards as well as future expansion decks that will feature different types of networks from different sectors. Thus, players can learn about a variety of different security concerns as they obtain future decks and expansion packs. The goal will be to distribute the majority of decks and boosters free-of-charge (thanks to corporate sponsorships) to school districts around the country. Our desire is to get these cards into the hands of as many individuals in public schools as possible. Everybody needs to know about security so, from our perspective, everybody needs a deck of Cyber Threat Defender cards!

We are always open to good ideas, so if you have an idea for a new card – we are ready to listen. If you have suggestions on how to improve the game, we are also very interested in hearing from you so play the game, take good notes, and tell us what you think.

We hope you have as much fun playing the game as we did in developing it. Let us hear from you!

Sincerely,

Gregory B. White, Ph.D.

Professor of Computer Science
Director, Center for Infrastructure Assurance and Security
The University of Texas at San Antonio
Introduction

In Cyber Threat Defender (CTD), the Cyber Security Collectable Card Game, your goal is to build your network as quickly as possible so you can “do more business” and gain more points. While you are doing this, you have to remember to defend your network because your opponent is going to try and disrupt your systems and network. For every attack there is a defense. For every defense there is an attack to get around it. The player with the most complete set of security defenses will be the one who is able to protect the critical systems and emerge victorious.

I. Preparation

a. You will need to have paper and pencil, or some other way to keep track of scores.

b. All players will need to have their own CTD deck of at least 50 cards.

c. Players may add to their CTD deck by way of booster cards. Customizing is allowed.

II. Game Objective

a. The game is played until a player obtains at least 30 points. If both players reach 30 points during the same round, then the player with the highest total wins. If both have the same total after reaching 30 points in the same round, the game continues until one player reaches 40 points. If a tie still exists, then the game is declared a draw.

b. Points are accumulated at the end of each round.

III. CTD Card Types

a. Asset Cards – These are your primary cards to build your network infrastructure. They represent the core of your physical assets you would encounter in a business or organization. Your starting cards, Desk Top and IP Network, are the foundation and can be expanded with a wireless network, which enables you to add Lap Top computers to your system.
b. Defense Cards – These cards are utilized to protect your network just as you would at home or in an organization. Defenses must be kept up to date. Failure to do so could have significant consequences for your network.

c. Attack Cards – These cards represent the various disreputable forces that exist on the internet today and not the player playing the card. Each of these cards can be protected against with proper use / employment of your defense cards.

d. Event Cards – These cards can help or hinder your network. They are various scenarios or events that take place in the real world. From “Budget Increases” that help improve
your system to “Power Outages” that leave you in the dark and your network unable to function. Carefully played, these cards can lead to a winning strategy.

Figure 4 Event Cards

IV. Parts of a Card

a. Below is a description of information found on a typical playing card.

Card Name

Card Type

Card Information

Card Abilities

Point Value

Figure 5 Parts of a Card

V. Setup

a. Each player places one (1) Desktop Computer and one (1) ISP Connection card face up on the table to start their network. (see figure 6)
b. This is your starting network which you must defend.

![Image of network cards]

Figure 6 A beginning System Network

c. Your goal is to build this network by adding additional assets and network components.

d. Players then shuffle the rest of their cards and deal themselves 7 cards. The remaining cards are placed face down in the Draw Pile. A Discard Pile will be placed next to the Draw Pile when a card is discarded.

e. Decide who will go first.

VI. A Players Turn

a. The player can play up to 3 cards of any combination of attack, defense, or asset. A maximum of only 2 of any one card type can be played in a turn. Event cards can be played at ANY time.

b. In Figure 7, the active player lays down his first card, which is the “Wireless Router” card and places it in line with his other asset cards. Although he gains no points from this card, the “Wireless Router” card must be played before a one (1) point value “Laptop” card can.

![Image of active player's cards]

Figure 7 Playing a Wireless Router Card
c. In Figure 8, the active player lays down his second card of the turn. This card is a “Firewall” defense card and he plays it on top of his “Desktop Computer” asset card thereby protecting the “network”.

![Figure 8 Playing a Firewall Card](image)

![Active Player](image)

![Opponent](image)

d. Figure 9, shows the active player’s third and final card played. This is a “Power Outage” event card, which is played on the opponent’s asset cards, thus causing the opponent to lose a turn.

![Figure 9 Playing a Power Outage Card](image)

![Active Player](image)

![Opponent](image)

e. At the end of the player’s turn, they discard cards from their hand until they have five (5) cards. The player then draws two (2) cards from their draw pile for a total of up to seven (7) cards in their hand. Thus, if a player has six (6) cards in their hand, they must discard one (1). If they have seven (7) they must discard two (2). The discard must be done BEFORE the selection of two (2) cards from the draw pile. See Figure 10.
f. If a player’s draw pile becomes empty, the player picks up and shuffles their discard pile then places it face down as the new draw pile.

VII. End of a Round

a. A Round consists of one turn for each player.

b. At the end of the Round, scores are tallied. Each player will add the points gained from cards in play.

c. In the example in Figure 11 the active player would gain 1 point from the Desktop Computer, 1 point from the ISP Connection and 1 point from the Laptop Computer that is connected to the Wireless Router. For this turn the active player is awarded 3 points.
VIII. Player Options

a. Critical System Failure Option: At the beginning of any turn, a player can declare “CRITICAL SYSTEM FAILURE”. The player then picks up all of their cards and has to start with just one ISP and one Desktop again. This is the player’s turn, no other cards may be played this turn. The opponent’s cards placed on the player are picked up and placed in the opponent’s discard pile.

b. An example of a Critical System Failure Option is in Figure 12. At this point if the player holds no defensive or event cards in their hand that could help resolve the various issues impacting his network system, it might be worth starting over again!

![Figure 12 Situation for using the Critical System Failure Option](image)

c. A player may choose to NOT play any cards during their turn. They must however discard and draw cards. Example; A player chooses not to play any cards, but they already have seven (7) cards in their hand. They must discard two cards and must draw two cards from their draw pile.

d. If your turn is skipped, or a card states you receive no points this round or turn, you do not receive any points for assets that you own this round. If you’ve played a card on an opponent that provides you points (such as a Phishing attack card), you may still gain these points at the end of the round as normal.

IX. Building A Custom Deck

To play CTD you need the starter deck of 54 cards. Players may “customize” their deck by collecting Booster Packs. Your deck should have a minimum of 50 cards but by selecting specific cards from the Booster Packs, players may add as many cards as they desire.
For a complete listing of cards, visit www.utsa.edu/CIAS/CTD/Card_List

For information on how to obtain additional decks or booster packs, visit www.utsa.edu/CIAS/CTD/cards

For possible sponsorship of a card or booster pack, visit www.utsa.edu/CIAS/CTD/sponsor

*Note to Security Professionals

In developing this game, we recognize that we have taken some liberties with how things actually work. We have attempted to keep true to the spirit of computer security but for playability reasons have slightly modified how things might actually work in reality. We believe, however, that the game is close enough that individuals playing the game will be able to gain some understanding of basic computer security concepts.